(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平9－153870

(43)公開日　平成９年(1997)６月10日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｈ　1/02			Ｈ０４Ｈ　1/02	Ｅ	
Ｈ０４Ｌ　9/32			Ｈ０４Ｌ　9/00	６７３Ｂ	
Ｈ０４Ｎ　7/167			Ｈ０４Ｎ　7/167	Ｚ	

審査請求　有　　請求項の数12　ＯＬ　（全 11 頁）

(21)出願番号　特願平8－210371

(22)出願日　平成８年(1996)８月９日

(31)優先権主張番号　１０００９６４

(32)優先日　1995年８月10日

(33)優先権主張国　オランダ（ＮＬ）

(71)出願人　591104918
コニンクリジケ　ピーティーティー　ネーダーランドエヌ　ブィー
KONINKIJKE PTT NEDERLAND NEAMLOZE VENNOOTSHAP
オランダ国　9726　エイシー　グローニゲン　ステーションズウエー　10

(72)発明者　ヨハン　バン　ティルバルグ
オランダ国　2719　ケイケイ　ゾエターメール　プラタッンホウト　64

(74)代理人　弁理士　斉藤　武彦

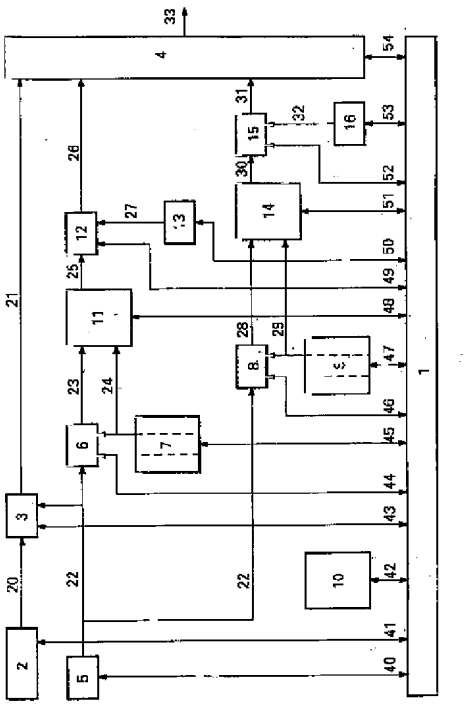
最終頁に続く

(54)【発明の名称】　受信装置のほか送信装置ならびに、暗号化／翻訳メッセージにより、情報へのアクセスを得る方法

(57)【要約】

【課題】　情報へのアクセスが、より能率的な方法で行われる方法を提供する。

【解決手段】　公認使用者ごとに、暗号化／翻訳メッセージにより、情報へのアクセスを得る周知の方法は、公認使用者のみが翻訳方法を行うので、使用者のみにより翻訳される暗号化メッセージを送信する。同じメッセージをすべての使用者に送信し、このメッセージは、使用者が公認されていなければ使用者に関連する暗号化方法により使用者ごとに暗号化され、使用者が公認されていれば暗号化されず、使用者は使用者に関連する翻訳方法を行わず他の使用者に関連する翻訳方法を行い、すべての使用者はこの同じメッセージを受信するが、公認使用者のみが暗号化メッセージを翻訳し、この翻訳されたメッセージにより情報へのアクセスを得ることができ、非公認使用者はそれらのためなお暗号化されたメッセージにより情報へのアクセスを得ることができず、この方法は能率的である。



【特許請求の範囲】
【請求項１】　暗号化／翻訳メッセージにより、公認使用者には情報へのアクセスを与え、非公認使用者には情報へのアクセスを与えない方法において、非公認使用者ごとに、前記非公認使用者に関連する暗号化方法によりメッセー非公認使用者ごとに、前記非公認使用者に関連する暗号化方法によりメッセージを暗号化する工程、
公認使用者ごとに、前記公認使用者に関連する暗号化方法によりメッセージを暗号化しない工程、使用者にメッセージを送信する工程、
各使用者が該使用者に関連する暗号化方法により暗号化されたメッセージを翻訳するため当該使用者に関連する翻訳方法を行わず、一方他の使用者に関連する暗号化方法により暗号化されたメッセージを翻訳するため前記他の使用者に関連する翻訳方法を行う様に、使用者によりメッセージを受信する工程、
少なくとも一人の非公認使用者の場合には、公認使用者ごとに、前記非公認使用者に関連する暗号化方法により暗号化されたメッセージを翻訳し、前記公認使用者により、翻訳メッセージによる情報へのアクセスを得る工程、
非公認使用者でない場合には、公認使用者ごとに、前記公認使用者ににより、非暗号化メッセージによる情報へのアクセスを得る工程、および非公認使用者ににより、暗号化メッセージによる情報へのアクセスを得ない工程を備えることを特徴とする方法。
【請求項２】情報は非暗号化メッセージにより暗号化され、非暗号化または翻訳メッセージによってのみ翻訳されることを特徴とする請求項１の方法。
【請求項３】メッセージは、もう１つの暗号化方法により送信前に暗号化され、受信後の暗号化メッセージは、もう１つの翻訳方法により翻訳されることを特徴とする請求項１または２の方法。
【請求項４】全数の使用者は多数の使用者群にわたり分配され、メッセージは使用者群ごとに送信されることを特徴とする請求項１、２または３の方法。
【請求項５】　公認使用者には情報へのアクセスを与え非公認使用者には情報へのアクセスを与えないためデータメッセージを使用者に送信する送信装置において、この送信装置は、
使用者ごとに、前記使用者に関連する暗号化方法によりデータメッセージを暗号化可能とする暗号化装置、およびデータメッセージに使用者確認信号を加算する加算装置を備え、
送信装置は、
使用者ごとに、非公認使用者の場合には第１値を有し公認使用者の場合には第２値を有する固有識別信号を発生する発生装置を備え、暗号化装置は、第１値を有する固有識別信号に応答して、前記非公認使用者に関連する暗号化方法によるデータメッセージを暗号化し、第２値を有する固有識別信号に応答して、前記公認使用者に関連する暗号化方法によるデータメッセージを暗号化しない、固有識別信号を使用者ごとに受信する制御入力を備えることを特徴とする送信装置。
【請求項６】　送信装置は、データメッセージにより、使用者に送信される情報を暗号化する暗号化手段を備えることを特徴とする請求項５の送信装置。
【請求項７】　送信装置は、もう１つの暗号化方法によりメッセージを暗号化する暗号化装置に結合されるもう１つの暗号化装置を備えることを特徴とする請求項５または６の送信装置。
【請求項８】　全数の使用者は多数の使用者群にわたり分配され、送信装置は使用者群ごとにデータメッセージを送信することを特徴とする請求項５、６または７の送信装置。
【請求項９】　公認使用者には情報へのアクセスを与え非公認使用者には情報へのアクセスを与えないデータメッセージを受信する受信装置において、受信装置は、
データメッセージの加えられる使用者確認信号を検出する検出装置を備え、受信装置は、
使用者確認信号から、非公認他の使用者の場合には第１値を有し公認他の使用者の場合には第２値を有する他の使用者に関連する少なくとも１つの固有識別信号を検出する検出装置に結合されるもう１つの検出装置、および第１値を有する他の使用者に関連する少なくとも１つの固有識別信号に応答して、前記非公認他の使用者に関連する翻訳方法によるデータメッセージを翻訳して、第２値を有する他の使用者に関連する少なくとも１つの固有識別信号に応答して、前記公認他の使用者に関連する翻訳方法によるデータメッセージを翻訳しない、もう１つの検出装置に結合される翻訳装置を備えることを特徴とする受信装置。
【請求項１０】　受信装置は、
翻訳または非暗号化データメッセージにより、受信情報を翻訳する翻訳手段を備えることを特徴とする請求項９の受信装置。
【請求項１１】　受信装置は、
もう１つの翻訳方法によりメッセージを翻訳する翻訳装置に結合されるもう１つの翻訳装置を備えることを特徴とする請求項９または１０の受信装置。
【請求項１２】　全数の使用者は多数の使用者群にわたり分配され、受信装置は、
ある使用者群に関連するデータメッセージを検出する検出手段を備えることを特徴とする請求項９、１０または１１の受信装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、暗号化／翻訳メッセージにより、公認使用者には情報へのアクセスを与え、非公認使用者には情報へのアクセスを与えない方法

に関する。
【０００２】
【従来の技術】このような方法は一般的な知識であり、つぎのように実行する。もし使用者が公認されていれば、使用者は暗号化メッセージを翻訳する翻訳方法を行うが、もし使用者が公認されていなければ、使用者は翻訳方法を行わない。その結果、公認使用者はメッセージを翻訳し、この翻訳メッセージにより使用者にある情報へのアクセスを与えるが、非公認使用者はメッセージを翻訳できず、その結果、使用者は情報へのアクセスを得られない。前記情報は、たとえば、メッセージに記録され、または、たとえば、使用者が翻訳メッセージを返した後のみに使用者に送信され、または、たとえば、暗号化状態で使用者に送信され、前記使用者は翻訳メッセージにもとずいてのみ暗号化情報を翻訳できる。
【０００３】このような方法は、とりわけ、公認使用者ごとに、メッセージが送信されねばならず、数ノードに接続される多くの使用者の場合には、多くのメッセージが順次送信されることになり、周知の方法は非能率的になり、各使用者は通過するすべての（暗号化）メッセージを付加的に見るという、欠点を有する。
【０００４】文献：
ＥＰ　０　６４１　１０３
１９９４年８月２１－２５日、米国カルフォルニア州サンタバーバラ、第１４年度国際暗号会議、暗号の進歩、クリプト’９４、ベニイ　コール、アモス　フィアットおよびモニ　ナオルによる”トレーシングトレーター”
１９９３年８月２３－２５日、米国カルフォルニア州サンタバーバラ、第１３年度国際暗号会議、暗号の進歩、クリプト’９３、アモス　フィアットおよびモニ　ナオルによる”放送暗号”
１９９２年、ＩＥＥＥプレス、グスタブスＪ．シモンズ編集、情報保全科学、”現代の暗号”
１９８２年、ジョン　ウイリー・アンド・サン、ウイリーインターサイエンス刊行物、カールＨ．メイヤーおよびステフェンＭ．メチアスによる、安全システムの設計および実施のガイド、”暗号術：コンピュターデータ安全の新次元”すべて文献はこの特許出願に組み込まれる。
【０００５】
【発明が解決しようとする課題】本発明の目的は、とりわけ、情報へのアクセスが、より能率的な方法で行われる、頭書に記載した種類の方法を提供することにある。
【０００６】
【課題を解決するための手段】この目的のため、本発明による方法は、非公認使用者ごとに、前記非公認使用者に関連する暗号化方法によりメッセージを暗号化する工程、公認使用者ごとに、前記公認使用者に関連する暗号化方法によりメッセージを暗号化しない工程、使用者にメッセージを送信する工程、各使用者が前記使用者に関連する暗号化方法により暗号化されたメッセージを翻訳するため前記使用者に関連する翻訳方法を行わず、一方他の使用者に関連する暗号化方法により暗号化されたメッセージを翻訳するため前記他の使用者に関連する翻訳方法を行い、使用者によりメッセージを受信する工程、少なくとも一人の非公認使用者の場合には、公認使用者が前記非公認使用者に関連する暗号化方法により暗号化されたメッセージを翻訳し、前記公認使用者により、翻訳メッセージによる情報へのアクセスを得る工程、非公認使用者でない場合には、公認使用者ごとが、前記公認使用者ににより、非暗号化メッセージによる情報へのアクセスを得る工程、および非公認使用者ににより、暗号化メッセージによる情報へのアクセスを得ない工程を備えることを特徴とする。
【０００７】同じメッセージを当該使用者に送信することによって、このメッセージは、前記使用者が公認されてなければ前記使用者に関連する暗号化方法により使用者ごとに暗号化され、前記使用者が公認されていれば前記使用者に関連する暗号化方法により暗号化されないものであり、当使用者はこの同じメッセージを受信するが、各使用者は前記使用者に関連する暗号化方法により暗号化されたメッセージを翻訳するため前記使用者に関連する翻訳方法を行わず、他の使用者に関連する暗号化方法により暗号化されたメッセージを翻訳するため前記他の使用者に関連する翻訳方法を行い、公認使用者のみが暗号化メッセージを翻訳できその翻訳されたメッセージにより情報へのアクセスを得ることができ、非公認使用者は、なお暗号化されたメッセージにより情報へのアクセスを得ることができず、非公認使用者でない場合には、もちろん、すべての公認使用者は非暗号化メッセージによる情報へのアクセスを得ることができある。その結果、同一のメッセージのみが当使用者に送信されねばならず、本発明による方法はきわめて能率的である。
【０００８】本発明は、とりわけ、つぎの暗号化メッセージを送信するつぎの使用者ごとよりもすべての使用者（公認使用者のみが、翻訳メッセージにより、情報へのアクセスを得ることができる）に同一の暗号化メッセージをかなり能率よく送信するという識見にもとずいている。
【０００９】周知の方法が非能率的であるという問題は同じメッセージを当使用者に送信することにより解決され、このメッセージは、使用者が公認されていなければ前記使用者に関連する暗号化方法により使用者ごとに暗号化され、前記使用者が公認されていれば暗号化されないものであり、この場合、各使用者は前記使用者に関連する暗号化方法により暗号化されたメッセージを翻訳するため前記使用者に関連する翻訳方法を行わされず、他の使用者に関連する暗号化方法により暗号化されたメッセージを翻訳するため前記他の使用者に関連する翻訳方法を行わなければならない。

【００１０】本発明による第１実施例は、情報は非暗号化メッセージにより暗号化され、非暗号化または翻訳メッセージによってのみ翻訳されることを特徴とする。
【００１１】非暗号化メッセージにより情報を暗号化することにより、このようにして暗号化された情報のみが、非暗号化または翻訳メッセージにより翻訳されることができ、公認使用者のみが前記情報へのアクセスを得る。
【００１２】本発明による第２実施例は、メッセージは、もう１つの暗号化方法により送信前に暗号化され、受信後の暗号化メッセージは、もう１つの翻訳方法により翻訳されることを特徴とする。
【００１３】もう１つの暗号化方法により送信前に暗号化することによって、もう１つの翻訳方法によりその翻訳を受信後、メッセージは、すべての当使用者が公認されていても、暗号化状態で常に送信されるので、安全性が得られる。
【００１４】本発明による第３実施例は、全数の使用者は多数の使用者群にわたり分配され、メッセージは使用者群ごとに送信されることを特徴とする。
【００１５】多数の使用者群にわたり全数の使用者を分配することにより、１つのメッセージは使用者群ごとに送信され、各使用者は明らかに、丁度使用者群と同じ多くの通過するメッセージを見るが、前記使用者はその使用者に関連するメッセージを翻訳するだけよく、また前記使用者は同じ使用者群に属するすべての他の使用者に関連する数の翻訳方法を行うだけでよい。
【００１６】本発明はさらに、公認使用者には情報へのアクセスを与え非公認使用者には情報へのアクセスを与えないためデータメッセージを使用者に送信する送信装置において、この送信装置は、使用者ごとに、前記使用者に関連する暗号化方法によりデータメッセージを暗号化可能とする暗号化装置、およびデータメッセージに使用者確認信号を加算する加算装置を備える、送信装置に関する。
【００１７】このような送信装置は一般的知識のものでつぎのように作動する。使用者ごと暗号化装置により、データメッセージは前記使用者に関連する暗号化方法により暗号化され、使用者確認信号は加算装置によりデータメッセージに加算され、暗号化データメッセージは前記使用者に送信される。使用者が公認されていれば、暗号化データメッセージを翻訳するため翻訳方法を実行するが、前記使用者が公認されていなければ、翻訳方法を実行しない。その結果、公認使用者はデータメッセージを翻訳し、翻訳データメッセージにより使用者にある情報へのアクセスをさせるが、非公認使用者はデータメッセージを翻訳できず、その結果情報へのアクセスを得られない。
【００１８】このような送信装置は、とりわけ、公認使用者ごとに１つのデータメッセージが送信されねばならず、数ノードに接続される多くの使用者の場合には、多くのデータメッセージが順次送信されることになり、装置全体が非能率的になり、さらに各使用者は、通過するすべての（暗号化）メッセージを見ると言う欠点がある。
【００１９】本発明の目的は、とりわけ、情報へのアクセスがより能率的に進められる、上記種類の送信装置を提供することにある。
【００２０】この目的のため、本発明による送信装置は、使用者ごとに、非公認使用者の場合には第１値を有し公認使用者の場合には第２値を有する固有識別信号を発生する発生装置を備えると共に、暗号化装置を備え、該暗号化装置は、第１値を有する固有識別信号に応答して、前記非公認使用者に関連する暗号化方法によるデータメッセージを暗号化し、第２値を有する固有識別信号に応答して、前記公認使用者に関連する暗号化方法によるデータメッセージを暗号化しない、固有識別信号を使用者ごとに受信する制御入力を備えることを特徴とする。
【００２１】発生装置により、非公認使用者の場合には第１値を有し、公認使用者の場合には第２値を有する使用者ごとの固有識別信号を発生することにより、暗号化装置は、第１値を有する固有識別信号に応答して、前記非公認使用者に関連する暗号化方法によるデータメッセージを暗号化し、第２値を有する固有識別信号に応答して、前記公認使用者に関連する暗号化方法によるデータメッセージを暗号化しない、固有識別信号を使用者ごとに受信する制御入力を備え、それで、同じデータメッセージは当使用者に送信され、このデータメッセージは、使用者が公認されていなければ使用者に関連する暗号化方法により使用者ごとに暗号化され、使用者が公認されていれば暗号化されず、当使用者はこの同じデータメッセージを受信する。各使用者が、使用者の暗号化方法により暗号化されたデータメッセージを翻訳するために使用者に関連する翻訳方法を行わず、他の使用者に関連する暗号化方法により暗号化されたデータメッセージを翻訳するために他の使用者に関連する翻訳方法を行えば、公認使用者のみが暗号化データを翻訳し、翻訳されたデータメッセージにより情報へのアクセスを得、非公認使用者はなお暗号化されたデータメッセージによる情報へのアクセスは得られず、非公認使用者でない場合には、もちろん、すべての公認使用者は非暗号化データメッセージにより情報へのアクセスを得ることができる。その結果、同一データメッセージのみが当使用者に送信されればよく、本発明による全体はきわめて能率がよい。
【００２２】本発明による送信装置の第１実施例は、送信装置がデータメッセージにより、使用者に送信される情報を暗号化する暗号化手段を備えることを特徴とする。
【００２３】暗号化手段により情報を暗号化することに

より、暗号化された情報は非暗号化または翻訳データメッセージによってのみ翻訳され、公認使用者のみが情報へのアクセスを得る。

【００２４】本発明による送信装置の第２実施例は、送信装置が、もう１つの暗号化方法によりメッセージを暗号化する暗号化装置に結合されるもう１つの暗号化装置を備えることを特徴とする。

【００２５】もう１つの暗号化装置により送信前にデータメッセージを暗号化することにより、受信後、もう１つの翻訳方法により翻訳されねばならず、データメッセージは、すべての当使用者が公認されていても暗号化状態で常に送信され、安全である。

【００２６】本発明による送信装置の第３実施例は、全数の使用者が多数の使用者群にわたり分配され、送信装置は使用者群ごとにデータメッセージを送信することを特徴とする。

【００２７】多数の使用者群にわたり全数の使用者を分配することにより、送信装置は使用者群ごとに１つのデータメッセージを送信し、各使用者は明らかに、使用者群と丁度同じ多くの通過するデータメッセージを見るが、前記使用者のみがその使用者群に関連するデータメッセージを翻訳すればよく、前記使用者のみが同じ使用者群に属するすべての他の使用者に関連する数の翻訳方法を行えばよい。

【００２８】本発明はさらに、公認使用者には情報へのアクセスを与え非公認使用者には情報へのアクセスを与えないデータメッセージを受信する受信装置において、受信装置は、データメッセージの加えられる使用者確認信号を検出する検出装置を備える、受信装置に関する。

【００２９】このような受信装置は一般的知識のもので、つぎのように作動する。使用者ごと、送信装置により、データメッセージは前記使用者に関連する翻訳方法により翻訳され、使用者確認信号は送信装置によりデータメッセージに加算され、暗号化し修正したデータメッセージは前記使用者に送信される。検出装置により、データメッセージに加えられる使用者確認信号が検出され、それににもとずいて、前記データメッセージが前記受信装置にたいするものかどうかが設定される。使用者が公認されていれば、受信装置は暗号化データメッセージを翻訳するために翻訳方法を行うが、使用者が公認されていなければ、受信装置は翻訳方法を行わない。その結果、公認使用者はデータメッセージを翻訳し、この翻訳データメッセージにより使用者にある情報へのアクセスをさせるが、非公認使用者はデータメッセージを翻訳できず、その結果使用者は情報へのアクセスはできない。

【００３０】このような受信装置は、とりわけ、公認使用者ごとに１つのデータメッセージが送信されねばならず、数ノードに接続される多くの使用者の場合には、多くのデータメッセージが順次送信されることになり、既知全体が非能率的になり、さらに各使用者は、通過するすべての（暗号化）メッセージを見ると言う欠点がある。

【００３１】本発明の他の目的は、とりわけ、情報へのアクセスがより能率的に進められる、上記種類の受信装置を提供することにある。

【００３２】この目的のため、本発明による受信装置は、使用者確認信号から、非公認他の使用者の場合には第１値を有し公認他の使用者の場合には第２値を有する他の使用者に関連する少なくとも１つの固有識別信号を検出する検出装置に結合されるもう１つの検出装置、および第１値を有する他の使用者に関連する少なくとも１つの固有識別信号に応答して、前記非公認他の使用者に関連する翻訳方法によるデータメッセージを翻訳して、第２値を有する他の使用者に関連する少なくとも１つの固有識別信号に応答して、前記公認他の使用者に関連する翻訳方法によるデータメッセージを翻訳しない、もう１つの検出装置に結合される翻訳装置を備えることを特徴とする。

【００３３】使用者確認信号からもう１つの検出装置により、非公認他の使用者の場合には第１値を有し公認他の使用者の場合には第２値を有する他の使用者に関連する少なくとも１つの固有識別信号を検出し、および第１値を有する他の使用者に関連する少なくとも１つの固有識別信号に応答する翻訳装置により、前記非公認他の使用者に関連する翻訳方法によるデータメッセージを翻訳して、第２値を有する他の使用者に関連する少なくとも１つの固有識別信号に応答して、前記公認他の使用者に関連する翻訳方法によるデータメッセージを翻訳しないことにより、同じデータメッセージは当使用者に送信され、このデータメッセージは使用者が公認されていなければ、使用者に関連する暗号化方法により使用者ごとに暗号化され、使用者が公認されていれば、暗号化されず、当使用者はこの同じデータメッセージを受信する。公認使用者のみが暗号化データメッセージを翻訳し、翻訳されたデータメッセージにより情報へのアクセスを得るが、非公認使用者でない場合には、もちろん、すべての公認使用者は非暗号化データメッセージにより情報へのアクセスを得る。その結果、同一のデータメッセージのみを当使用者に送信すればよく、本発明による全体はきわめて能率的である。

【００３４】本発明による受信装置の第１実施例は、翻訳または非暗号化データメッセージにより、受信情報を翻訳する翻訳手段を備えることを特徴とする。

【００３５】送信装置により情報を暗号化することにより、このように暗号化された情報のみが翻訳手段により翻訳され、公認使用者のみが情報へのアクセスを得る。

【００３６】本発明による受信装置の第２実施例は、もう１つの翻訳方法によりメッセージを翻訳する翻訳装置に結合される、もう１つの翻訳装置を備えることを特徴

とする。
【００３７】データメッセージが送信装置により送信前に暗号化されれば、受信後、もう１つの翻訳装置により翻訳されねばならず、データメッセージは、すべての当使用者が公認されていても暗号化状態で常に送信され、安全である。
【００３８】本発明による受信装置の第３実施例は、全数の使用者は多数の使用者群にわたり分配され、受信装置は、ある使用者群に関連するデータメッセージを検出する検出手段を備えることを特徴とする。
【００３９】全数の使用者を多数の使用者群にわたり分配することにより、送信装置は使用者群ごとに１つのデータメッセージを送信し、各使用者は明らかに使用者群と丁度同じ多くの通過するデータメッセージを見るが、前記使用者は、検出手段により、検出し、使用者群に関連するデータメッセージのみを翻訳せねばならず、使用者は、同じ使用者群に属するすべての他の使用者に関連する数の翻訳方法のみを行わねばならない。
【００４０】ＥＰ－０６４１１０３は選択送信システムにおけるキーを分配する方法および装置を開示する。この場合、各受信者はそれ自身のキーでなくすべての他の受信者のキーを扱う。組み合わせキーによる送信者は暗号化情報を送信し、この組み合わせキーはすべての非公認受信者に属するキーのモジュロー２付加により得られる。非公認受信者はそれら自身のキーを扱わないので、どの受信者が非公認であるかを知って、組み合わせキーを模倣できないが、公認受信者は、どの受信者が非公認であるかを知って、組み合わせキーを模倣し、その結果、暗号化情報は、組み合わせキーにより、公認受信者のみにより翻訳できる。その欠点は、とりわけ、授権の付加／除去により、情報が暗号化される変型組み合わせキーとなり、その結果、前記授権の付加／除去は発生する大きな技術的問題なしに極めて限られた数のモーメントでのみ行うか、または任意のモーメントで生ずるかであり、大きな技術的問題を含む。この特許には本発明による方法も本発明による装置のいずれも開示されていない。
【００４１】
【実施例】以下、本発明を、図に示す典型実施例を参照して詳細に説明する。ここで、図１は本発明による方法に適用する本発明による送信装置を示し、図２は本発明の方法に適用する本発明による受信装置を示す。
【００４２】図１に示す本発明による送信装置は、制御接続部４１により、プロセッサー１に結合され、その出力が、接続部２０により、暗号化手段３の第１入力に結合される情報源２を備える。さらにまた図１に示す本発明による送信装置は、制御接続部４により、プロセッサー１に結合され、その出力が、接続部２２により、暗号化手段３の第２入力と、第１暗号化装置６の第１入力と、第２暗号化装置６の第１入力とに結合されるメッセージメモリ５を備える。プロセッサーメモリ１０は、制御接続部４２により、プロセッサー１に結合され；暗号化手段３は、制御接続部４３により、プロセッサー１に結合され；第１暗号化装置６は、制御接続部４４により、プロセッサー１に結合され；第２暗号化装置８は、制御接続部４６により、プロセッサー１に結合される。暗号化手段３の出力は、接続部２１により、マルチプレクサー４の第１入力に結合される。第１暗号化装置６の第１入力は、接続部２４を介して、制御接続部４５によりプロセッサー１に結合される第１テーブルメモリ７の出力に接続される。第２暗号化装置８の第２入力は、接続部２９により、制御接続部４７によりプロセッサー１にに結合される第２テーブルメモリ９の接続される。第１暗号化装置６の出力は、接続部２３により、制御接続部４８によりプロセッサー１に結合され、その第２入力が接続部２４により第１テーブルメモリ７のの出力に接続される第１加算装置１１の第１入力に結合される。第２暗号化装置８の出力は、接続部２８により、制御接続部５１によりプロセッサー１に結合され、その第２入力が接続部２９により第２テーブルメモリ９の出力に接続される第２加算装置１４の第１入力に結合される。第１加算装置１１の出力は、接続部２５により、制御接続部４９によりプロセッサー１に結合され、その第２入力が接続部２７により、制御接続部５０によりプロセッサー１に結合される第１コードメモリ１３のの出力に接続される第３暗号化装置１２の第１入力に結合される。第２加算装置１４の出力は、接続部３０により、制御接続部５２によりプロセッサー１に結合され、その第２入力が接続部３２により、制御接続部５３によりプロセッサー１に結合される第２コードメモリ１６のの出力に接続される第４暗号化装置１５の第１入力に結合される。第３暗号化装置１２の出力は、接続部２６によりマルチプレクサー４の第２入力に結合され、第４暗号化装置１５の出力は、接続部３１により、その出力が接続部３３に接続され、制御接続部５４によりプロセッサー１に結合されるマルチプレクサー４の第３入力に結合される。
【００４３】図１に示す送信装置の作動は次の通りである。送信されるペイーＴＶビデオ信号は情報源２に格納される。その送信前に、公認の人または第１使用者群に属する使用者でない人は第１テーブルメモリ７に記録され、公認の人または第２使用者群に属する使用者でない人は第２テーブルメモリ９に記録される。この目的のため、両テーブルメモリ７と９各々は３つのコラム、すなわち、使用者識別を格納する行ごとの第１コラム、公認の人または関連使用者でない人を格納する行ごとの第２コラム、および関連使用者に結合される暗号化方法を格納する行ごとの第３コラムを有する。一般に、第１および第３コラムに格納されるデータは既に存在するかまたは長期間格納されるが、第２コラムに必要なデータは送信されるペイーＴＶビデオ信号ごとに設定され両テーブ

ルメモリ７と９にロードされねばならない。これは制御接続部４５、４７およびプロセッサー１により行われる。送信されるペイーＴＶビデオ信号ごとに、制御接続部４０およびプロセッサー１により、メッセージメモリ５にロードされるメッセージがさらに設定される。

【００４４】メッセージメモリ５は、制御接続部４０により、プロセッサー１から生ずる指令信号を受信して、それに応答して、接続部２２により暗号化手段３、第１暗号化装置６および第１暗号化装置８に送られる格納メッセージを発生する。暗号化手段３はさらに、接続部２０により、制御接続部４１により受信される指令信号に応答して情報源２により送信される情報源２から生じかつプロセッサー１から生ずるペイーＴＶビデオ信号を受信し、制御接続部４３により受信される制御信号の制御の下にメッセージにもとずきかつプロセッサー１から生ずる前記ペイーＴＶビデオ信号を暗号化して、その後暗号化ビデオ信号は接続部２１によりマルチプレクサー４に送られる。

【００４５】第１テーブルメモリ７は、制御接続部４５により、プロセッサー１から生ずる指令信号を受信し、引き続き、それに応答して、第１群識別および行ごと（または使用者識別ごと）に格納されているデータ（の一部）を発生し、第１群識別、すべての使用者識別および行ごと（または使用者識別ごと）第１と第２コラムに格納される使用者公認が、接続部２４により、第１加算装置１１に送られる一方、第３コラムに格納される暗号化方法のうち、非公認使用者に関連する暗号化方法のみが接続部２４により第１暗号化装置６に送られる。制御接続部４４により受信され、プロセッサー１から発する制御信号の制御の下、第１暗号化装置６は、非公認使用者に関連する暗号化方法により、たとえば、前記暗号化方法をある順序でメッセージに引き続き与えることにより受信メッセージを暗号化する。その後、第１暗号化装置６は、プロセッサー１の制御の下、暗号化されたメッセージを第１の仕方で接続部２３により第１加算装置１１に送る。第１加算装置１１は、プロセッサー１から生じ制御接続部４８により受信される制御信号に応答して、第１の仕方で暗号化されたメッセージを、第１テーブルメモリ７に格納される第１群識別、すべての使用者識別および使用者公認と組み合わせ、プロセッサー１の制御の下、組み合わせ全体を接続部２５により第３暗号化装置１２に送る。第１コードメモリ１３は、制御接続部５０により、プロセッサー１から発する指令信号を受信して、それに応答して、接続部２７により第３暗号化装置１２に送られる第１コードを発生する。制御接続部４９により受信されプロセッサー１から生ずる制御信号の制御の下、第３暗号化装置１２は第１コードにもとずいて到来組み合わせ全体を暗号化する。その後、第３暗号化装置１２はプロセッサー１の制御の下、第１コードにより暗号化された全体を接続部２６によりマルチプレクサー４に送る。

【００４６】第２テーブルメモリ９は、制御接続部４７により、プロセッサー１から生ずる指令信号を受信し、引き続き、それに応答して、第２群識別および行ごと（または使用者識別ごと）格納されるデータ（の一部）を発生し、第２群識別、すべての使用者識別および行ごと（または使用者識別ごと）に第１と第２コラムに格納される使用者公認が、接続部２９により、第２加算装置１４に送られる一方、第３コラムに格納される暗号化方法のうち、非公認使用者に関連する暗号化方法のみが接続部２９により第２暗号化装置８に送られる。制御接続部４６により受信され、プロセッサー１から発する制御信号の制御の下、第２暗号化装置８は、非公認使用者に関連する暗号化方法により、たとえば、前記暗号化方法をある順序でメッセージに引き続き与えることにより受信メッセージを暗号化する。その後、第２暗号化装置８は、プロセッサー１の制御の下、暗号化されたメッセージを第２の仕方で接続部２８により第２加算装置１４に送る。第２加算装置１４は、プロセッサー１から生じ制御接続部５１により受信される制御信号に応答して、第２の仕方で暗号化されたメッセージを、第２テーブルメモリ９に格納される第２群識別、すべての使用者識別および使用者公認と組み合わせ、プロセッサー１の制御の下、組み合わせ全体を接続部３０により第４暗号化装置１５に送る。第２コードメモリ１６は、制御接続部５３により、プロセッサー１から発する指令信号を受信して、それに応答して、接続部２７により第４暗号化装置１２に送られる第２コードを発生する。制御接続部５２により受信されプロセッサー１から生ずる制御信号の制御の下、第４暗号化装置１５は第２コードにもとずいて到来した組み合わせ全体を暗号化する。その後、第４暗号化装置１５はプロセッサー１の制御の下、第２コードにより暗号化された全体を接続部３１によりマルチプレクサー４に送る。

【００４７】制御接続部５４により受信され、プロセッサー１から生ずる制御信号の制御の下、マルチプレクサー４は暗号化ビデオ信号を、第１コードにより暗号化された全体および第２コードにより暗号化された全体と組み合わせた後、その結果を、接続部３３により、少なくとも第１および第２使用者群に属する使用者に送信される。

【００４８】本発明による図２に示す受信装置は、その入力が接続部３３に接続され、制御接続部１４０によりプロセッサー１００に結合されるデマルチプレクサー１０１を備える。デマルチプレクサー１０１の第１出力は、接続部１２０により、制御接続部１４７によりプロセッサー１００に結合される翻訳手段１０２の第１入力に結合される。翻訳手段１０２の出力はたとえばテレビジョンセット等情報プロセッサーに結合するため接続部１２１に接続され、翻訳手段１０２の第２入力は接続部

１２７により第１翻訳装置１０７の出力に接続される。第１翻訳装置１０７の第１入力は接続部１２５により分割装置１０５の第１出力に結合され、第１翻訳装置１０７の第２の入力は接続部１２８により、制御接続部１４６によりプロセッサー１００に結合される第３テーブルメモリ１０８の出力に接続される。制御接続部１４５により第１翻訳装置１０７はプロセッサー１００に結合される。分割装置１０５の第２出力は、接続部１２６により、制御接続部１４４によりプロセッサー１００に結合されるデータルメモリ１０６の入力に結合される。分割装置１０５の入力は、接続部１２４により、第２翻訳装置１０３の出力に接続され、一方分割装置１０５は制御接続部１４３により、プロセッサー１００に結合される。第２翻訳装置１０３の第１入力は接続部１２２によりデマルチプレクサー１０１の第２出力に結合され、第２入力は接続部１２３により、制御接続部１４２によりプロセッサー１００に結合される第３コードメモリ１０４の出力に接続される。制御接続部１４１により、第２暗号化装置１０３はプロセッサー１００に結合される。

【００４９】図２に示す受信装置の作動は次の通りである。ここで、この受信装置は第１使用者群に属する公認使用者に関連するものと想定する（送信装置では、メッセージは前記公認使用者に関連する暗号化方法により暗号化されないで、他の非公認使用者に関連する暗号化方法により多分暗号化される）。制御接続部１４０により受信されプロセッサー１００から生ずる制御信号の制御の下、デマルチプレクサー１０１は暗号化ビデオ信号を、第１コードにより暗号化された全体および第２コードにより暗号化された全体から分離した後、暗号化ビデオ信号は、接続部１２０により翻訳手段１０２に送られ、第１コードにより暗号化された全体は接続部１２２により第２翻訳装置１０３に送られる。第３コードメモリ１０４は制御接続１４２により、プロセッサー１００から生ずる指令信号を受信し、それに応答して、接続部１２３により第２翻訳装置１０３に送られる第３コードを発生する。制御接続部１４１により受信されプロセッサー１００から生ずる制御信号の制御の下、第２翻訳装置１０３は第３コードにもとずいて第１コードにより翻訳された全体を翻訳する。一般に、この場合、第１コードと第３コードとは等しい。つぎに、第２翻訳装置１０３は、プロセッサー１００の制御の下、第３コードにより翻訳された全体を、接続部１２４により分割装置１０５に送る。

【００５０】分割装置１０５は、プロセッサー１００から生じ制御接続部１４３により受信される制御信号に応答して、第３コードにより翻訳された全体を、一方で、第１の仕方で暗号化されたメッセージに、他方で第１群識別、すべての使用者識別および使用者公認に分割し、プロセッサー１００の制御の下、第１の仕方で暗号化されたメッセージを第１翻訳装置１０７に送り、プロセッサー１００の制御の下第１群識別、すべての使用者識別および使用者公認を接続部１２６によりデータメモリ１０６に送る。プロセッサー１００は、制御接続部１４４により、第１群識別が（たとえば、テーブルメモリ１０８に格納され、制御接続部１４６によりプロセッサー１００に送られる（第１群識別を一致せねばならない）第３群識別と比較することによって）データメモリ１０６に格納されていることを検出し、その結果、前記データが全く前記受信装置に意図されていることが設定される。

【００５１】第３テーブルメモリ１０８は３つのコラム、すなわち、使用者識別を格納する行ごとの第１コラム、公認の人または関連使用者でない人を格納する行ごとの第２コラム、および関連使用者に結合される暗号化方法を格納する行ごとの第３コラムを有する。一般に、第１および第３コラムに格納されるデータは既に存在するかまたは長期間格納されるが、第２コラムに必要なデータは送信されるペイーＴＶビデオ信号ごとに設定され、テーブルメモリ１０８にロードされねばならない。これは、プロセッサー１００の制御の下、データメモリ１０６に格納される使用者識別および使用者公認を制御接続１４４により、プロセッサー１００により、および制御接続１４６により第３テーブルメモリ１０８に送ることにより行われる。

【００５２】第３テーブルメモリ１０８は、制御接続部１４６により、プロセッサー１から生ずる指令信号を受信して、それに応答して第３コラムに格納される行ごと（または使用者識別ごと）にデータ（の一部）を受信する一方、第３コラムに格納される翻訳方法のうち、非公認使用者に関連する翻訳公報のみが、接続部１２８により、第１翻訳装置１０７に送られる。制御接続部１４５により受信されプロセッサー１００から生ずる制御信号の制御の下、第１翻訳装置１０７は、非公認使用者に関連する翻訳方法による暗号化メッセージを、たとえば、（送信装置とは逆の）ある順序で前記翻訳方法にメッセージを引き続き与えることによって、翻訳する。つぎに、第１翻訳装置１０７は、プロセッサー１００の制御の下、翻訳メッセージを、接続部１２７により翻訳手段１０２に送る。

【００５３】翻訳手段１０２は、制御接続部１４７により、プロセッサー１００から生ずる制御信号を受信し、それに応答して、接続部１２７により受信される翻訳メッセージにもとずいて暗号化ビデオ信号を翻訳した後、元のペイーＴＶビデオ信号は接続部によりまた、たとえば、テレビジョンセットにより観察される。

【００５４】他の（第２の）使用者群に意図される、第２コードにより送信装置で暗号化される全体に関する限り、図２に示す受信装置の作動には、少なくとも３つの作動がある。第１に、デマルチプレクサー１０１は、たとえば、ある時間間隔を無視することにより既に選択

し、それで第２コードにより暗号化される全体はデマルチプレクサー１０１を通らない。第２に、第２コードにより送信装置で暗号化される全体は、たとえば、やがて、第１コードにより暗号化される全体から分離されるので、デマルチプレクサー１０１を通り、さらに、第１コードにより暗号化される全体が提供された後いつか、第２翻訳装置１０３に提供される一方、第２コードは第３コードメモリに格納される第３コードとは異なるので、この時、ここでは正しい翻訳が行われず、その結果分割装置１０５および（または）データメモリ１０６は意味のないことに対処しなければならない。

【００５５】第３に、第１コードにより暗号化される全体は、たとえば、やがて、第１コードにより暗号化される全体から分離されるので、デマルチプレクサー１０１を通り、さらに、第１コードにより暗号化される全体が提供された後いつか、第２翻訳装置１０３に提供される一方、この時第２コードは第３コードメモリに格納される第３コードとは異ならないので、ここでは、正しい翻訳が行われる。分割装置１０５は、プロセッサー１００から生じ制御接続部１４３により受信される制御信号に応答して、第３コードにより翻訳された全体を、一方で、第２の仕方で暗号化されたメッセージに、他方で第２群識別、すべての使用者識別および使用者公認に分割し、分割装置１０５は、プロセッサー１００の制御の下、第２の仕方で暗号化されたメッセージを第１翻訳装置１０７に送り、さらに分割装置１０５は、プロセッサー１００の制御の下、第２群識別、すべての使用者識別および使用者公認を接続部１２６によりデータメモリ１０６に送る。プロセッサー１００は、制御接続部１４４により、他の（第２群識別が（たとえば、テーブルメモリ１０８に格納され、制御接続部１４６により、プロセッサー１００に送られる（第１群識別を一致せねばならない）第３群識別と比較することによって）データメモリ１０６に格納されていることを検出し、その結果、前記データが前記受信装置に意図されていないことが設定される。勿論、前記検出とは別に、第２の仕方で暗号化されたメッセージは一般に、第１翻訳装置１０７により正しい方法で翻訳され得ない。

【００５６】前記受信装置が第１使用者群に属する使用者、この時は非公認に関連するとすれば（送信装置では、メッセージは非公認使用者に関連する暗号化方法により暗号化され、多分さらに他の非公認使用者に関連する暗号化方法により暗号化されるので、前記他の使用者群の残りの公認使用者に関連する暗号化方法により暗号化されない）、図２に示す受信装置の作動は、下記を除いて上記に従う。

【００５７】第３テーブルメモリ１０８は、制御接続部１４６により、プロセッサー１００から生ずる指令信号を受信し、それに応答して、引き続き発生し、接続部１２８により、第１翻訳装置１０７に、受信装置を管理する非公認使用者に関連する翻訳方法を除いて、非公認使用者に関連する第３コラムに格納される翻訳方法お送る。前記１つの翻訳方法を発生しないのは、たとえば、前記テーブルメモリ１０８に存在しない前記翻訳方法の結果、または、すべてこれは、明らかに存在するが反対に前記テーブルメモリ１０８で非活動である前記１つの翻訳方法の結果である。この時、第１翻訳装置１０７は、前記翻訳方法の１つが得られないので、非公認使用者に関連する翻訳方法による暗号化メッセージの翻訳は果たせない。その結果、もう１つの暗号化メッセージは、暗号化ビデオ信号が翻訳できない翻訳手段１０２に送られる。

【００５８】ペイーＴＶビデオ信号がアナログ信号であれば、暗号化手段３と翻訳手段１０２は当業者に周知のフィルムコーダーとフィルムデコーダーである。マルチプレクサー４とデマルチプレクサー１０１は、たとえば、ビデオ信号とディジタルテレックス信号（また暗号化メッセージと使用者識別等）が組み合わされる、いわゆるテレビジョンチップである。ペイーＴＶビデオ信号がディジタル信号であれば、暗号化手段３と翻訳手段１０２は、たとえば、各々、たとえば、たとえば６４ビットキーワードの関数として６４ビット入力ワードを６４ビット出力ワードに変換する、いわゆる、暗号チップと翻訳チップである。暗号化装置６、８、１２、１５と翻訳装置１０３、１０７は、また暗号チップと翻訳チップにより実現される。この場合、従って、メッセージ、暗号化方法および翻訳方法は、いわゆるキーからなる。

【００５９】”情報”の概念はできるだけ広い意味を持つように解釈すべきである。したがって、ペイーＴＶビデオ信号に関するだけでなく、またオプションとして、たとえば、ケーブル網により、航空情報を航空人の家庭に送信することがあり、たとえば、航空人の第１部分は完全に公認され、航空人の第２、第３部分は各々、航空情報の異なる部分についてのみ公認される。これとは別に情報は、たとえば、電気メインにより、使用者の家庭に送信され、この場合、公認使用者のみのボイラーおよび（または）サンスクリーンが駆動されうる。また、”情報へのアクセスを与える、暗号化／翻訳メッセージにより”は、情報源とメッセージ源は地理的に分離されると共に一致するが、ある場合の情報はメッセージに完全に記録されさえされるので（翻訳または非暗号化メッセージは、全部また一部が、情報と一致する）、できるだけ広い意味を持つように解釈すべきである。

【００６０】使用者が受信装置を購入または借りる場合には、前記受信装置は一般に、（たとえば、データメモリ１０６および（または）テーブルメモリ１０８に格納される）使用者識別と（一般にコードメモリ１０４に格納される）標準翻訳方法および（または）標準キーを既に備えている。そこで、前記受信装置に送信される第１メッセージは（一般にコードメモリ１３および（また

は）１６に格納される）標準翻訳方法および（または）標準キーにより、送信装置に暗号化されねばならず、受信装置に翻訳された後、受信装置に、たとえば、（一般に、コードメモリ１０４に格納される）新コード、群識別、および、（たとえば、データメモリ１０６および（または）テーブルメモリ１０８に格納される）同じ群に属する使用者の使用者識別、ならびに（たとえば、テーブルメモリ１０８に格納される）関連翻訳方法および（または）キー等翻訳メッセージに存在するデータがロードされる。また、受信装置に既に格納されたデータの拡張および（または）修正および（または）変型は一般に１つ以上のメッセージにより行われる。この場合、メッセージには表示を備え、この表示は、前記メッセージが主として、翻訳装置１０７および（または）翻訳手段１０２を意図することを表示し、またはメッセージが主としてデータの調節を意図することを表示し、この表示は分割装置１０５および（または）データメモリ１０６および（または）プロセッサー１００により検出されねばならない。

【図面の簡単な説明】

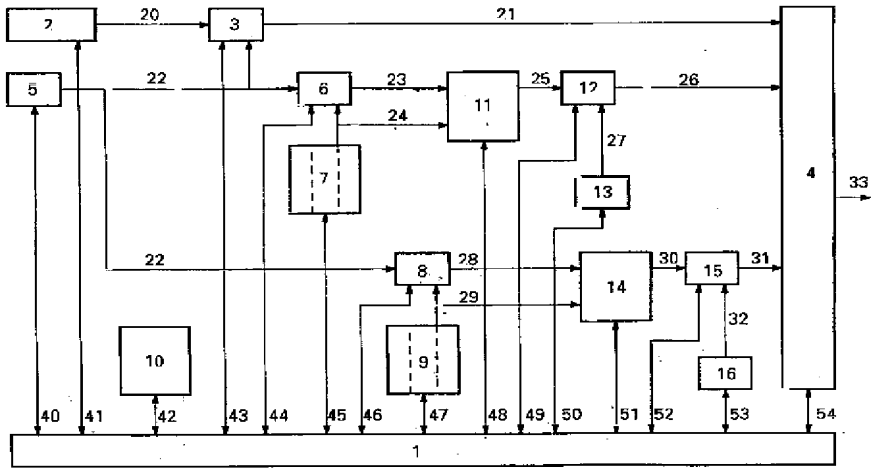
【図１】本発明による方法に適用する本発明による送信装置を示す。

【図２】本発明による方法に適用する本発明による受信装置を示す。

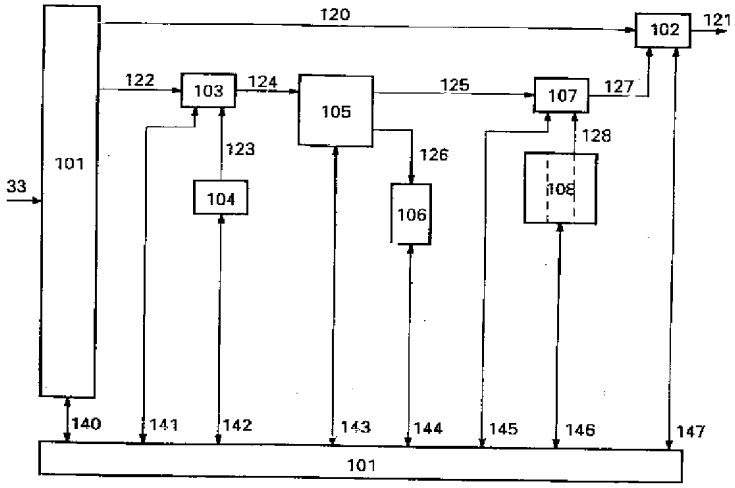
【符号の説明】

１、１００…プロセッサー
２…情報源
３…暗号化手段
４…マルチプレクサー
５…メッセージメモリ
６…第１暗号化装置
７…第１テーブルメモリ
８…第２暗号化装置
９…第２テーブルメモリ
１０…プロセッサーメモリ
１１…第１加算装置
１２…第３テーブルメモリ
１３…第１コードメモリ
１４…第２加算装置
１５…第４テーブルメモリ
１６…第２コードメモリ
２０－３３、１２０－１２５、１２７、１２８…接続部
４０－５４、１４０－１４７…制御接続部
１０１…デマルチプレクサー
１０２…翻訳手段
１０３…第２翻訳装置
１０４…第３コードメモリ
１０５…分割装置
１０６…データメモリ
１０７…第１翻訳装置
１０８…第３テーブルメモリ

【図１】



【図２】



フロントページの続き

(72)発明者　アンドリース　ピーター　ヘクストラ
オランダ国　2252　ケイエム　ボールショーテン　ルーイス　デ　コリングニラーン　11